1. (Four Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which said user computer cannot rewrite, and said medium personal number is used for generating a decryption key for decrypting said encrypted electronic data in said user computer; and

permission information which includes [a] the decryption key encrypted in a manner that is generated independent from a specific apparatus number for a specific computer, and generated based upon said medium personal number.

6. (Four Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at

least the medium personal number is written onto the storage medium in an un-rewritable form which said user computer cannot rewrite, and said medium personal number is used for generating an encrypted permission information in said vendor computer; and

permission information encrypted in a manner that is generated independent from a specific apparatus number for a specific computer and generated based upon said medium personal number, wherein the permission information enables decryption of the encrypted electronic data.


11. (Four Times Amended) A storage medium accessed by a vendor computer and a user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic data;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

encrypted permission information that is generated independent from a specific apparatus number for a specific computer and generated based upon said medium personal number;

wherein at least the medium personal number is written onto the storage medium in an unrewritable form which a user computer cannot rewrite, and wherein said encrypted permission information enables decryption of the encrypted electronic data.

17. (Four Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein the medium personal number is written onto the storage medium in an un-rewritable form which a user storage reading apparatus cannot rewrite;

encrypted electronic [information] data; and

information which is encrypted based on said medium personal number and is encrypted independent from a specific apparatus number for a specific computer and said medium personal number is used for generating a decryption key for decrypting said encrypted electronic data in said user computer.


18. (Four Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

encrypted electronic [information] data;

a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user storage reading apparatus cannot rewrite, and

said medium personal number is used for decrypting said encrypted electronic [information] data; and

information which is encrypted based on said medium personal number and is encrypted independent from a specific apparatus number for a specific computer.

19. (Four Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic [information] data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a first storage area for storing encrypted electronic [information] data, the encrypted electronic [information includes] data including electronic [information] data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is

particularly personal for each storage medium and is different from a medium personal

number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the

encrypted decryption key is generated based upon the medium personal number and the

encrypted decryption key is generated independent from the specific apparatus number

for the specific first computer,

wherein the encrypted decryption key in the third storage area enables decryption

of the encrypted electronic data in the first storage area by the second computer.


23. (Four Times Amended) A storage medium accessible from a first computer

which encrypts a decryption key based upon a medium personal number and independent

from a specific apparatus number for a specific first computer and which stores the

encrypted decryption key onto the storage medium and which encrypts electronic

[information] data based upon the decryption key and which stores the encrypted

electronic [information] data onto the storage medium, and accessible from a plurality of

second computers which decrypt the encrypted decryption key stored on the storage

medium based upon the medium personal number and independent from a specific

apparatus number for a specific second computer and which decrypt encrypted electronic

[information] data stored on the storage medium based upon the encrypted decryption

key that has been decrypted based on the medium personal number and independent from

the specific apparatus number for the specific second computer, the storage medium

comprising:

a first storage area for storing encrypted electronic [information] data, the encrypted electronic [information includes] data includes electronic [information] data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific first computer,

wherein the encrypted decryption key in the third storage area enables decryption of the encrypted electronic data in the first storage area by the second computer.

24. (Four Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a first storage area for storing encrypted electronic [information] data, the encrypted electronic [information includes] data including electronic [information] data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area enables decryption of the encrypted electronic data in the first storage area by a user computer.


25. (Four Times Amended)  A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic [information] data based upon the encrypted decryption key and which stores the encrypted electronic [information] data onto the storage medium, the storage medium comprising:

a first storage area for storing encrypted electronic [information] data, the encrypted electronic [information includes] data including electronic [information] data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

- 7 -

a third storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area enables decryption of the encrypted electronic data in the first storage area by a user computer.

26. (Four Times Amended) A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon a medium personal number and independent from a specific apparatus number for a specific computer, and which decrypt encrypted electronic [information] data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer [in a particular computer], the storage medium comprising:

a first storage area for storing encrypted electronic [information] data, the encrypted electronic [information includes] data including electronic [information] data encrypted based upon the decryption key;

a second storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the <u>encrypted</u> decryption key is generated based upon the medium personal number and the <u>encrypted</u> decryption key is generated independent from the specific apparatus number for the specific computer,

<u>wherein the encrypted decryption key in the third storage area enables decryption of the encrypted electronic data in the first storage area by a user computer.</u>

27. (Four Times Amended) A storage medium accessible from [different computers] <u>a vendor computer and a user computer</u> at different times, the storage medium comprising:

a first storage area for storing encrypted electronic [information] <u>data</u>, the encrypted electronic [information includes] <u>data including</u> electronic [information] <u>data</u> encrypted based upon a decryption key;

a second storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the <u>encrypted</u> decryption key is generated based upon the medium personal number and the <u>encrypted</u> decryption key is generated independent from a specific apparatus number for a specific computer,

wherein the encrypted decryption key in the third storage area enables decryption

of the encrypted electronic data in the first storage area by the user computer.


28. (Four Times Amended) A storage medium accessed by a vendor computer

and a user computer, said storage medium[,] comprising:

a first storage area for storing encrypted electronic [information] data, the

encrypted electronic [information includes] data including electronic [information] data

encrypted based upon a decryption key;

a second storage area for storing a medium personal number, which is un-

rewritable, wherein the medium personal number is particularly personal for each storage

medium and is different from a medium personal number of another storage medium; and

a third storage area for storing an encrypted decryption key, wherein the encrypted

decryption key is generated based upon the medium personal number and the encrypted

decryption key is generated independent from a specific apparatus number for a specific

computer,

wherein the encrypted decryption key in the third storage area enables decryption

of the encrypted electronic data in the first storage area by the user computer.


29. (Four Times Amended) A storage medium accessible from a first computer

which encrypts a decryption key based upon a medium personal number and independent

from a specific apparatus number for a specific first computer and which stores the

encrypted decryption key onto the storage medium, and accessible from a plurality of

second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic [information] data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data and the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific first computer, and wherein the encrypted decryption key enables decryption of the encrypted electronic data by the second computer.


33. (Four Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic [information] data based upon the decryption key and which stores the encrypted electronic [information] data onto the storage medium, and accessible from a plurality of

second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic [information] data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data and the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific second computer, and wherein the encrypted decryption key enables decryption of the encrypted electronic data by the second computer.


34. (Four Times Amended)  A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; [and]

a storage area for storing the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from the specific apparatus number for the specific computer; and

a storage area for storing encrypted electronic data which is accessible after the decryption key has been decrypted, wherein said decryption key enables decryption of the encrypted electronic data by a user computer.

35. (Three Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic [information] data based upon the decryption key and which stores the encrypted electronic [information] data onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted electronic data and the encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal

number and the encrypted decryption key is generated independent from the specific

apparatus number for the specific computer, and wherein the encrypted decryption key

enables decryption of the encrypted electronic data by a user computer.

36. (Four Times Amended)  A storage medium accessible from a plurality of

computers which decrypt an encrypted decryption key stored on the storage medium, the

encrypted decryption key being based upon the medium personal number and

independent from a specific apparatus number for a specific computer and which decrypt

encrypted electronic [information] data stored on the storage medium based upon the

decryption key that has been decrypted based on the medium personal number and

independent from the specific apparatus number for the specific computer in a particular

computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable

from the computers, wherein the medium personal number is particularly personal for

each storage medium and is different from a medium personal number of another storage

medium; [and]

a storage area for storing the encrypted decryption key, wherein the encrypted

decryption key is generated based upon the medium personal number and the encrypted

decryption key is generated independent from the specific apparatus number for the

specific computer; and

a storage area for storing encrypted electronic data which is accessible after the decryption key has been decrypted, wherein said decryption key enables decryption of the encrypted electronic data by a user computer.

37. (Four Times Amended) A storage medium accessible from [different computers] a vendor computer and a user computer at different times, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable from the computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing an encrypted decryption key, wherein the encrypted decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer; and

a storage area for storing encrypted electronic data which is accessible after the decryption key has been decrypted, wherein said decryption key enables decryption of the encrypted electronic data by the user computer.

38. (Four Times Amended) A storage medium accessed by a vendor computer and a user computer, said storage medium, comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing an encrypted decryption key, wherein the <u>encrypted</u> decryption key is generated based upon the medium personal number and the encrypted decryption key is generated independent from a specific apparatus number for a specific computer; and

a storage area for storing <u>encrypted</u> electronic data which is accessible after the decryption key has been decrypted, <u>wherein said decryption key enables decryption of the encrypted electronic data by the user computer</u>.

39. (Four Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium, and accessible from a plurality of second computers which decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic [information] <u>data</u> stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted [information] <u>electronic data</u> which includes [information] <u>data</u> encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific first computer,

<u>wherein the encrypted electronic data is decrypted from the second computer.</u>

43. (Four Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific first computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic [information] <u>data</u> based upon the decryption key and which stores the encrypted electronic [information] <u>data</u> onto the storage medium, and accessible from a plurality of second computers which [the] decrypt the encrypted decryption key stored on the storage medium based upon the medium personal number and independent from a specific apparatus number for a specific second computer and which decrypt encrypted electronic [information] <u>data</u> stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific second computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable from at least the second computers, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted [information] <u>electronic data</u> which includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific second computer,

<u>wherein the encrypted electronic data is encrypted from the second computer.</u>

44. (Four Times Amended) A storage medium accessible from a [first] <u>vendor</u> computer <u>and a user computer, where the vendor</u> computer [which] encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted [information] <u>electronic data</u> [which] <u>wherein</u> <u>the encrypted electronic data</u> includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer.

45. (Four Times Amended) A storage medium accessible from a first computer which encrypts a decryption key based upon a medium personal number and independent from a specific apparatus number for a specific computer and which stores the encrypted decryption key onto the storage medium and which encrypts electronic [information] data based upon the decryption key and which stores the encrypted electronic [information] data onto the storage medium, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted [information] electronic data [which] wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the encrypted electronic data is decrypted from a user computer.


46. (Four Times Amended) A storage medium accessible from a plurality of computers which decrypt an encrypted decryption key stored on the storage medium, the encrypted decryption key being based upon the medium personal number and independent from a specific apparatus number for a specific computer and which decrypt encrypted electronic [information] data stored on the storage medium based upon the decryption key that has been decrypted based on the medium personal number and

independent from the specific apparatus number for the specific computer in a particular

computer, comprising:

a storage area for storing the medium personal number, which is un-rewritable

from the computers, wherein the medium personal number is particularly personal for

each storage medium and is different from a medium personal number of another storage

medium; and

a storage area for storing encrypted [information] <u>electronic data</u> [which] <u>wherein</u>

<u>the encrypted electronic data</u> includes information encrypted based upon the medium

personal number and encrypted independent from the specific apparatus number for the

specific computer,

<u>wherein the encrypted electronic data is decrypted from a user computer.</u>


47. (Four Times Amended) A storage medium accessible from different

computers at different times, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable from

the computers, wherein the medium personal number is particularly personal for each

storage medium and is different from a medium personal number of another storage

medium;

a storage area for storing encrypted [information] <u>electronic data</u> which includes

information encrypted based upon the medium personal number and encrypted

independent from a specific apparatus number for a specific computer; and

a storage area for storing electronic data which is accessible after the encrypted [information] electronic data has been decrypted,

wherein the medium personal number enables decryption of the encrypted electronic data from a user computer.

48. (Three Times Amended) A storage medium accessed by a vendor computer and a user computer, said storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

a storage area for storing encrypted [information] electronic data which includes information encrypted based upon the medium personal number and encrypted independent from a specific apparatus number for a specific computer; and

a storage area for storing electronic data which is accessible after the encrypted [information] electronic data has been decrypted,

wherein the medium personal number enables decryption of the encrypted electronic data from the user computer.

49. (Four Times Amended) A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium,

and accessed in a manner such that the encrypted decryption key stored on the storage medium is decrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer and that encrypted electronic [information] data stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted [information] electronic data [which] wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key enables decryption of the encrypted electronic data from the user computer.


53. (Four Times Amended) A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is decrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and the encrypted decryption key is stored onto the storage medium and that electronic [information] data is encrypted based upon the decryption key and the encrypted electronic [information] data is stored onto the storage medium, and accessed

in a manner such that the encrypted decryption key stored on the storage medium is decrypted based upon the medium personal number and independent from the specific apparatus number for the specific computer and that the encrypted electronic information stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer in a particular second computer in different time, the storage medium comprising:

a storage area for storing a medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted [information] electronic data [which] wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key enables decryption of the encrypted electronic data from the user computer.


54. (Four Times Amended) A storage medium accessed by a vendor computer and a user computer in a manner such that a decryption key is encrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and that the encrypted decryption key is stored onto the storage medium, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable,

wherein the medium personal number is particularly personal for each storage medium

and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted [information] electronic data [which] wherein

the encrypted electronic data includes information encrypted based upon the medium

personal number and encrypted independent from the specific apparatus number for the

specific computer,

wherein the decryption key enables decryption of the encrypted electronic data

from the user computer.


55. (Four Times Amended) A storage medium accessed by a vendor computer

and a user computer in a manner such that a decryption key is encrypted based upon a

medium personal number and independent from a specific apparatus number for a

specific computer and the encrypted decryption key is stored onto the storage medium

and that electronic [information] data is encrypted based upon the decryption key and the

encrypted electronic [information] data is stored onto the storage medium, the storage

medium comprising:

a storage area for storing the medium personal number, which is un-rewritable,

wherein the medium personal number is particularly personal for each storage medium

and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted [information] electronic data [which] wherein

the encrypted electronic data includes information encrypted based upon the medium

personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key enables decryption of the encrypted electronic data from the user computer.


56. (Four Times Amended)  A storage medium accessed by a vendor computer and a user computer in a manner such that an encrypted decryption key stored on the storage medium is decrypted based upon a medium personal number and independent from a specific apparatus number for a specific computer and encrypted electronic [information] data stored on the storage medium is decrypted based upon the decryption key that has been decrypted based on the medium personal number and independent from the specific apparatus number for the specific computer, the storage medium comprising:

a storage area for storing the medium personal number, which is un-rewritable, wherein the medium personal number is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

a storage area for storing encrypted [information] electronic data [which] wherein the encrypted electronic data includes information encrypted based upon the medium personal number and encrypted independent from the specific apparatus number for the specific computer,

wherein the decryption key enables decryption of the encrypted electronic data from the user computer.

111. (Three Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user computer cannot change; and

an area storing permission information which includes a decryption key encrypted in a manner that is independent from a specific apparatus number for a specific computer and based upon said medium personal number, wherein said permission information enables decryption of the encrypted electronic data from the user computer.


112. (Three Times Amended) A storage medium accessed by a vendor computer and user computer, said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user computer cannot rewrite; and

[an area storing] wherein decryption of the encrypted electronic data with the user computer is enabled by permission information which is encrypted in a manner that is independent from a specific apparatus number for a specific computer and based upon said medium personal number.

113. (Four Times Amended) A storage medium accessed by a vendor computer and a user computer said storage medium for storing information readable by said user computer, said storage medium comprising:

an area storing encrypted electronic data;

an area storing a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium; and

[an area storing encrypted] wherein decryption of the encrypted electronic data with the user computer is enabled by permission information that is encrypted independent from a specific apparatus number for a specific computer;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which a user computer cannot rewrite.

119. (Four Times Amended) A storage medium readable by a vendor computer and a user computer, said storage medium comprising:

data representing a medium personal number;

encrypted <u>electronic</u> data; and

first data that is based on the medium personal number and encrypted independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium, and wherein the first data is used by the <u>user</u> computer to decrypt the encrypted <u>electronic</u> data.

123. (Four Times Amended) A storage medium readable by [different computers] <u>a vendor computer and a user computer</u> at different times, the storage medium comprising:

data representing a medium personal number;

encrypted <u>electronic</u> data; and

first data that is based on the medium personal number and encrypted independent from a specific apparatus number for a specific computer, wherein the medium personal number is un-rewritable and particularly personal for each storage medium and is different from a medium personal number of another storage medium, and wherein the first data is used by the <u>user</u> computer to decrypt the encrypted <u>electronic</u> data.

124. (Three Times Amended)  A storage medium for storing data for access and processing by a [storage reading apparatus] vendor computer and a user computer, said storage medium comprising:

a medium personal number storage area including a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium, wherein the medium personal number is written onto the storage medium in an un-rewritable form which a user storage reading apparatus cannot rewrite;

an electronic information storage area including encrypted electronic [information] data; and

[an information storage area including information which is] the encrypted electronic data is decrypted from the user computer based upon an encrypted decryption key which has been encrypted based on said medium personal number and encrypted independent from a specific apparatus number for a specific computer.


125. (Three Times Amended)  A storage medium for storing data for access and processing by a [user storage reading apparatus] vendor computer and a user computer, said storage medium comprising:

an encrypted electronic [information] data storage area including encrypted electronic [information] data;

a medium personal number storage area including a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user storage reading apparatus cannot rewrite, and said medium personal number [is used for] enables decrypting of said encrypted electronic [information] data from the user computer; and

[an information storage area including] wherein the encrypted electronic data is decrypted from the user computer based upon information which is encrypted based on said medium personal number and encrypted independent from a specific apparatus number for a specific computer.

125. (Three Times Amended) A storage medium for storing data for access and processing by a vendor computer and a user computer, said storage medium comprising:

an encrypted electronic data storage area including encrypted electronic data;

a medium personal number storage area including a medium personal number which is particularly personal for each storage medium and is different from a medium personal number of another storage medium;

wherein at least the medium personal number is written onto the storage medium in an un-rewritable form which the user storage reading apparatus cannot rewrite, and said medium personal number enables decrypting of said encrypted electronic data from the user computer; and

wherein the encrypted electronic data is decrypted from the user computer based upon information which is encrypted based on said medium personal number and encrypted independent from a specific apparatus number for a specific computer.

## REMARKS

The Official Action dated November 4, 2002 has been received and carefully noted. The period for response having been extended from February 4, 2003 until March 4, 2003 by the attached Petition for Extension of Time, the above amendments and the following remarks are submitted as a full and complete response thereto.

As a preliminary matter, applicants appreciate the Examiner's courtesy in conducting the interview of January 23, 2003. The productive discussion during that

interview led to agreement regarding virtually all of the rejections which were set forth in

the Official Action of November 4, 2002. The amendments set forth above, therefore,

contain all of the amendments which were discussed during the interview, and includes

additional amendments in order to further satisfy concerns on certain issues. No new

matter has been added by these amendments. It is respectfully submitted that claims 1-56

and 111-125 are now in condition for allowance and reissue. The following remarks,

therefore, are merely formalizing the discussion set forth in the interview.

Claims 1-56 and 111-125 were rejected under 35 USC § 101, on the grounds that

the claimed invention was directed to non-statutory subject matter. The Official Action

took the position that although the original claims had been amended to recite "a vendor

computer and a user computer", this was not a sufficient amendment to place the claims

in compliance with United States patent practice. However, applicants respectfully

submit that all of claims 1-56 and 111-125 recite sufficiently functional descriptive

elements so as to be in compliance with 35 USC § 101, and the corresponding guidelines

set forth in MPEP § 2106. For example, claim 1 recites a storage medium comprising

encrypted electronic data, a medium personal number which is particularly personal for

each storage medium and is different from a medium personal number of another storage

medium, wherein at least the medium personal number is written onto the storage

medium in an un-rewritable form which the user computer cannot rewrite. Claim 1

further recites that the medium personal number is used for generating a decryption key

for decrypting the encrypted electronic data in the user computer. Therefore, the

functional language regarding the medium personal number provides a specific function of the medium personal number with respect to the encrypted electronic data. Claim 1 additionally recites permission information which includes the decryption key with the decryption key encrypted in a manner that is generated independent from a specific apparatus number for a specific computer, and is generated based upon the medium personal number. All of the presently pending claims recite similar functional relationships between the areas of the storage medium which are recited in the various claims, and/or the storage medium and the user computer, which places the claims clearly in compliance with 35 USC § 101. MPEP § 2106, § II, paragraph A, explains that "only when the claim is devoid of any limitation to a practical application in the technological arts should it be rejected under 35 USC § 101." As discussed above and as discussed during the interview, all of the claims clearly recite the practical application of decryption of encrypted data, and/or enabling access to a storage area by a computer. As preliminarily agreed during the interview, it is respectfully requested that the rejection under 35 USC § 101 be withdrawn.

Claims 24-28, 34-39, 44-56, and 119-125 were rejected under 35 USC § 251 as being an improper recapture of broadened subject matter. The Official Action took the position that the original patent application included amendments to issued independent claims 1, 6 and 11 regarding an addition to the preamble of "accessed by a vendor computer and user computer," and other aspects. The Official Action took the position that since claims 24-28, 34-39, 44-56 and 119-125 did not include that limitation, this

was an improper recapture. Applicants respectfully submit, however, that the amendments to issued claims 1, 6 and 11 were not submitted as narrowing amendments, and were not submitted to overcome a prior art rejection. This aspect was added to the claims in order to attempt to overcome a previous rejection under 35 USC § 101. However, as discussed above (and in view of changes regarding rejections under 35 USC § 101), the above amendments were likely unnecessary at the time. In view, however, of the fact that these amendments were not narrowing, and were not for the purpose of overcoming prior art, the omission of these phrases from claims in this reissue application is not an improper recapture under 35 USC § 251. However, in an effort to expedite the allowance of this application, all of currently pending claims 1-56 and 111-125 have been amended either to recite that the storage medium is accessible from a first computer and a second computer, a vendor computer and a user computer, etc. As discussed during the interview, it is believed that the above explanation and these amendments are sufficient to warrant withdrawal of the above-discussed recapture rejection.

Claims 1-10 were rejected under 35 USC § 251 as being an improper recapture due to the omission thereof of information regarding a decryption key, or an encrypted permission key. It is respectfully submitted that all of claims 1-16 have been amended to include all of the elements which were included in the claims in the issued patent. Each claim, therefore, refers to the same information regarding a decryption key which was contained in the previous claims. This rejection, therefore, is now moot.

Claims 17-20, 24, 25, 39-46, 49-56 and 119-125 are rejected under 35 USC § 112, second paragraph, as being indefinite. The Official Action took the position that there were unclear recitations in these claims regarding "encrypted information" and "encrypted data". In order to be more consistent throughout the claims, the term "encrypted electronic data" has been used throughout, where applicable. Therefore, there is no confusion between any encrypted electronic information, encrypted electronic data, permission information, etc. As preliminarily agreed during the interview, these amendments should be sufficient to withdraw this rejection.

Claims 29-33, 35, 39-47, 49-56, and 124 were rejected under 35 USC § 251 as being directed to an invention that was not disclosed in the original patent. In the Official Action, it was indicated that the claims did not recite a third storage area on a storage medium. However, as discussed during the interview, Figure 13 of the original patent illustrates a configuration with storage medium 11 contains medium number 12 and encrypted software 15. This can be viewed in contrast to Figures 2 and 3, which indicate storage medium 1 or 11 containing medium number 12, permission information 13, and encrypted electronic data 14 or encrypted software 15. It is respectfully submitted, therefore, that the invention as now recited in all of claims 1-56 and 111-125 was disclosed as part of the original invention in the original issued patent.

Once again, applicants appreciate the Examiner's courtesy in conducting the interview on January 23, 2003. Applicants respectfully submit that the amendments discussed herein are consistent with the amendments discussed during the interview, with
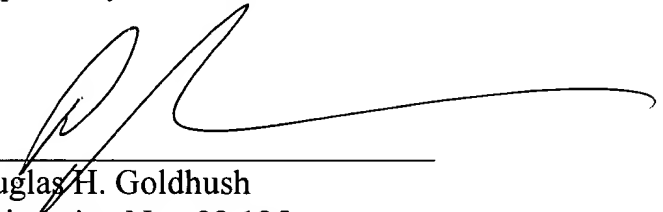
the exception of some additional amendments having been made at the recommendation of Examiner Barron.

It is respectfully requested that claims 1-56 and 111-125 be found allowable, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Douglas H. Goldhush
Registration No. 33,125

**Customer No. 32294**
SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14th Floor
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DHG:scc

Enclosures: Marked-up Copy of Amended Claims